## REMARKS

The Examiner objected to claims 2, 4, 10-11, 17, 20, 22-23, 26 and 27 to as being dependent on rejected on base claims.

The Examiner also rejected claims 1, 3, 5-6, 9, 12-13, 18-19, and 21 under 35 U.S.C. 102(b) as being anticipated by Messmer. The Examiner also rejected claims 7-8, 14-16, 24 and 25 under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Hill et al.

Applicant contends that Messmer or Messmer in view of Hill do not anticipate or render obvious the claims as previously submitted. Nevertheless, Applicant has amended the claims to take into consideration the examiner's indication of allowable subject matter. Applicant reserves its right to file a continuation application on the canceled subject matter (independent claims prior to amendment).

The Examiner also stated that:

> **The reasons why the claims are objected to is because the control center of prior art does not eliminate block or request the victim center to set up filters. The prior art of record monitors for intrusions, the center monitors and gives the victim center ways in which to handle the attacks.**

Although Applicant generally agrees with this statement of allowance, Applicant notes that the claims are objected to because they depend on rejected base claims, but the examiner believes that the subject matter of the objected to claims is not found in the combination of references. Applicant also notes that the canceled subject matter (independent claims prior to amendment) is neither described nor suggested by the references. Applicant's claims were patentable over Hill alone, and Messmer with Hill does not cure the deficiencies of Hill or the other cited art.

Applicant has canceled objected to claims 2, 10, 20 and 23 and included the limitations of those objected to claims into their respective independent claims 1, 9, 18 and 21, thus making those claims, as well as, all of Applicant's remaining claims allowable.

Applicant has enclosed an information disclosure statement that cites references from other applications of the current assignee.

The claims as amended are allowable over these references since the references do not suggest in combination the features of a control center to coordinate thwarting attacks ***, the control center *** to receive data from a plurality of monitors *** with the monitors sending data *** over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from and *** a process that executes on the computer system to analyze the data *** and an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.

For example, Mell discusses in 3.0 Vulnerable Systems:

> **In addition, if an attacker floods communication channel on which an IDS node is residing, the IDS node is cut off from the rest of the virtual IDS network. These vulnerability exists regardless of the protections implemented on the IDS node. One solution to this problem is to provide IDSs a separate and protected communication channel for their operation. This solution works well but is very costly, as separate cables must be run for the IDS system. Our solution using mobile agents provides a solution to this problem without having to have separate protected communication channels for IDS nodes. However, our solution has its own set of requirements and assumptions.**

At the most, Mell is cumulative with the teachings of Messmer, e.g., "to provide IDSs a separate and protected communication channel for their operation." Moreover, Mell teaches away from providing "IDSs a separate and protected communication channel for their operation," as being too costly and proposes a solution of using mobile agents. Therefore, it is not suggested to combine the teachings of Mell with Hill, Messmer nor the other cited art.

Further, Mell is directed to distributed hierarchical systems. Mell discusses:

> **In these systems, an attacker can amputate portions of an IDS by taking out statically located command and control hosts. The resulting IDS has reduced detection capability at best and is completely disabled at worst. This inherent weakness in modern distributed IDSs is due to their hierarchical nature. For example, if one shuts down the root node of a distributed hierarchical application it ceases to function. However, organizing IDS components into a hierarchical structure is an ideal way to detect and respond to attacks in large networks. The majority of IDSs that scale to large networks are organized in a hierarchical fashion because this structure provides many performance and organizational advantages. The alternative, a completely distributed non-hierarchical IDS structure has been tried by several research IDSs but has proven inefficient both in detecting distributed attacks and in quickly reporting attacks.**

Applicant's claim 1 is directed to an arrangement with a plurality of monitors and a control center, not the hierarchy described by Mell. Mell does not suggest the feature of a

control center to coordinate thwarting attacks on a victim data center that is coupled to a network. Mell also does not suggest the feature of an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.

Applicant has enclosed an Information Disclosure Statement. Applicant contends that the claims are allowable over the art in the IDS and the art of record.

Accordingly, the application is in condition for allowance and such action is respectfully requested.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 7/19/07

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110-2804
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21069395.doc